AMENDMENTS TO THE CLAIMS

Claim 1 (Currently Amended) A computer system for securely and reliably manipulating target information by adding two or more integers, the computer system comprising:

a memory unit operable to store a program composed of a plurality of instructions; ~~and~~

a processor operable to (i) fetch each instruction ~~in turn~~ from the program stored in the memory unit, ~~and~~, (ii) decode and execute each fetched instruction, and (iii) securely and reliably manipulate the target information by executing security processing on the target information; ~~wherein~~

~~the program includes~~

a conversion unit operable to control, according to an instruction of the program, ~~conversion instruction set to have~~ the processor to first generate elements belonging to a group G by implementing a power operation which performs exponentiation to ~~in the group G using~~ each of the two or more integers, ~~integer,~~ the group G being based on an integer residue ring Z/nZ, where (i) $n = p_1^{m1} \times p_2^{m2} \times \ldots \times p_k^{mk}$, (ii) each of $m_1, m_2, \ldots, m_k$ is an integer being no less than one, (iii) k is an integer being greater than one, (iv) each of $p_1, p_2, \ldots, p_k$ denotes mutually differing prime numbers, (v) Z denotes an integer ring, (vi) the integer residue ring Z/nZ is composed of values that are congruent modulo m, and (vii) x denotes multiplication;

a multiplication unit operable to control, according to an instruction of the program, ~~an operation instruction set to have~~ the processor to second generate an operation value by implementing a multiplication ~~basic operation other than addition~~ using all of the ~~generated~~ elements first generated by the processor according to the control of the conversion unit; and, ~~and~~

an inverse conversion unit operable to control, according to an instruction of the program, ~~instruction set to have~~ the processor to third generate a sum value of the two or more integers by implementing, in the group G or a proper subgroup S of the group G, an inverse power operation on the operation value second generated by the processor according to the control of the multiplication unit, the inverse power operation including solving a discrete logarithm in the subgroup S, wherein:

the processor executes the security processing on the target information according to the control of the conversion unit, the multiplication unit, and the inverse conversion unit to add two or more integers;

the security processing includes (i) encrypting or decrypting the target information based on key information, the encrypting or decrypting being accomplished by adding the key information or second key information obtained from the key information to the target information or second target information obtained from the target information, the adding being executed according to the control of the conversion unit, the multiplication unit, and the inverse conversion unit and (ii) implementing a digital signature or digital signature verification on the target information based on the key information, the implementation of the digital signature or the digital signature verification being accomplished by adding the key information or second key information obtained from the key information to the target information or second target information obtained from the target information, the adding being executed according to the control of the conversion unit, the multiplication unit, and the inverse conversion unit.

Claims 2-5 (Cancelled)

Claim 6 (Currently Amended) The computer system of Claim 1 ~~5~~, wherein the inverse conversion unit is operable to control, according to an instruction of the program, ~~instruction set includes instructions to have~~ the processor use a Chinese Remainder Theorem to solve a discrete logarithm problem in each ~~of the~~ multiplicative group ~~groups of~~ Z/Zp_1^{m1}, Z/Zp_2^{m2}, ..., Z/Zp_k^{mk} ~~Z/Zp1, Z/Zp2,... , Z/Zpk, which use the primes p1, p2,... ,pk, respectively~~.

Claims 7-9 (Cancelled)

Claim 10 (Currently Amended) The computer system of Claim 1, ~~2,~~ wherein:

the subgroup S is an anomalous elliptic curve group; ~~group,~~

the ~~conversion~~ multiplication unit is operable to control, according to an instruction of the program, ~~instruction set has~~ the processor to implement a multiplication on the elliptic curve using each of the two or more integers ~~integer, and~~; and

the computer system further includes an addition unit operable to control, according to an instruction of the program, the processor to ~~operation instruction set has the processor~~ implement an addition of ~~the~~ each element ~~elements~~ on the elliptic curve.

Claim 11 (Currently Amended) The computer system of Claim 1, ~~2,~~ wherein:

the group G is a direct product of two anomalous elliptic curve groups resulting in an elliptical curve; ~~groups,~~

the ~~conversion instruction set has~~ multiplication unit is operable to control, according to an instruction of the program, the processor to implement a multiplication on the elliptic curve using each of the two or more integers ~~integer, and~~; and

the computer system further includes an addition unit operable to control, according to an instruction of the program, ~~operation instruction set has~~ the processor to implement an addition of ~~the~~ generated elements on the elliptic curve.

Claim 12 (Currently Amended) The computer system of Claim 1, ~~2,~~ wherein the inverse conversion unit is operable to control, according to an instruction of the program, ~~instruction set has~~ the processor to (i) store a plurality of exponents, each exponent being in correspondence with a value raised to a power using a respective exponent, and (ii) find the inverse of the power operation by searching ~~the correspondences~~ each correspondence between an exponent and a corresponding value raised to a power using a respective exponent.

Claim 13 (Currently Amended) The computer system of Claim 1, ~~2,~~ wherein the inverse conversion unit is operable to control ~~instruction set includes a reduction portion to have~~ the processor reduce each element belonging to the group G to an element belonging to the subgroup S.

Claim 14 (Cancelled)

Claim 15 (Currently Amended) The computer system of Claim 1, ~~14,~~ wherein the ~~encryption~~ encrypting is based on a shared key encryption algorithm, and the ~~decryption~~ decrypting is based on a shared key decryption algorithm.

Claim 16 (Cancelled)

Claim 17 (Currently Amended) The computer system of Claim 1, ~~2,~~ wherein the processor and the memory are integrated on an IC card.

Claim 18 (Currently Amended) ~~An addition~~A method ~~used~~ of using a computer system including a memory unit and a processor ~~for~~ to securely and reliably manipulate target information by adding two or more integers ~~using a computer system that includes a memory unit and a processor~~, the ~~addition~~ method of using the computer system comprising ~~steps of~~:

storing, in the memory unit, a program composed of a plurality of instructions;

controlling ~~a conversion step to cause~~, according to an instruction of the program, the processor to first generate elements belonging to a group G by implementing a power operation which performs exponentiation to ~~in the group G using~~ each of the two or more integers ~~integer~~, the group G being based on an integer residue ring Z/nZ, where (i) $n = p_1^{m1} \times p_2^{m2} \times \ldots \times p_k^{mk}$, (ii) each of $m_1, m_2, \ldots, m_k$ is an integer being no less than one, (iii) k is an integer being greater than one, (iv) each of $p_1, p_2, \ldots, p_k$ denotes mutually differing prime numbers, (v) Z denotes an integer ring, (vi) the integer residue ring Z/nZ is composed of values that are congruent modulo m, and (vii) x denotes multiplication;

controlling ~~an operation step to cause~~, according to an instruction of the program, the processor to second generate an operation value by implementing a multiplication ~~basic operation other than addition~~ using all of the ~~generated~~ elements generated by the controlling of the processor to first generate elements; ~~, and~~

controlling ~~an inverse conversion step to cause~~, according to an instruction of the program, the processor to third generate a sum value of the two or more integers by implementing, in the group G or a proper subgroup S of the group G, an inverse power operation on the operation value generated by the controlling of the processor to second generate the operation value, the inverse power operation including solving a discrete logarithm in the subgroup S; and

securely and reliably manipulating target information by controlling the processor to execute security processing on the target information according to (i) the controlling of the processor to first generate elements, (ii) the controlling of the processor to second generate the

operation value, and (iii) the controlling of the processor to third generate the sum value,

wherein the security processing includes (i) encrypting or decrypting the target information based on key information, the encrypting or decrypting being accomplished by adding the key information or second key information obtained from the key information to the target information or second target information obtained from the target information, and (ii) implementing a digital signature or digital signature verification on the target information, the implementing of the digital signature or the digital signature verification being accomplished by adding the key information or second key information obtained from the key information to the target information or second target information obtained from the target information.

Claim 19 (Currently Amended) A computer-readable storage medium having a computer program stored thereon, the computer program for securely and reliably manipulating target information by adding two or more integers, the computer program causing a computer including a memory unit and a processor to execute a method comprising:~~, including:~~

storing, in the memory unit, a program composed of a plurality of instructions;

controlling~~a conversion instruction set for generating~~, according to an instruction of the program, the processor to first generate elements belonging to a group G by implementing a power operation which performs exponentiation to~~in the group G using~~ each of the two or more integers~~integer~~, the group G being based on an integer residue ring Z/nZ, where (i) $n = p_1^{m1} \times p_2^{m2} \times \ldots \times p_k^{mk}$, (ii) each of $m_1, m_2, \ldots, m_k$ is an integer being no less than one, (iii) k is an integer being greater than one, (iv) each of $p_1, p_2, \ldots, p_k$ denotes mutually differing prime numbers, (v) Z denotes an integer ring, (vi) the integer residue ring Z/nZ is composed of values that are congruent modulo m, and (vii) x denotes multiplication;

controlling~~an operation instruction set for generating~~, according to an instruction of the program, the processor to second generate an operation value by implementing a multiplication-~~basic operation other than addition~~ using all of the~~generated~~ elements generated by the controlling of the processor to first generate elements;~~, and~~

controlling~~an inverse conversion instruction set for generating~~, according to an instruction of the program, the processor to third generate a sum value of the two or more integers by implementing, in the group G or a proper subgroup S of the group G, an inverse power operation

on the operation value generated by the controlling of the processor to second generate the operation value, the inverse power operation including solving a discrete logarithm in the subgroup S; and

securely and reliably manipulating target information by controlling the processor to execute security processing on the target information according to (i) the controlling of the processor to first generate elements, (ii) the controlling of the processor to second generate the operation value, and (iii) the controlling of the processor to third generate the sum value,

wherein the security processing includes (i) encrypting or decrypting the target information based on key information, the encrypting or decrypting being accomplished by adding the key information or second key information obtained from the key information to the target information or second target information obtained from the target information, and (ii) implementing a digital signature or digital signature verification on the target information, the implementing of the digital signature or the digital signature verification being accomplished by adding the key information or second key information obtained from the key information to the target information or second target information obtained from the target information.

Claims 20-22 (Cancelled)